UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,757	11/15/2001	Sami Kilkkila	602.357USW1	3174

7590 06/15/2004

SQUIRE SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive
14th Floor
Tysons Corner, VA 22182-2700

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	12

DATE MAILED: 06/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/007,757	KILKKILA, SAMI	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Rowland (US 6,405, 318)

a. *Referring to claim 1:*

i. Rowland teaches:

(1) defining in the computer system access right profiles having individual command rights to the operating system of the computer system **[i.e., referring to Figure 1, a local controller function 6, that is for "defining in the computer system access right profiles having individual command rights to the operating system of the computer system". Furthermore, referring to Figure 8, a flow diagram of the control function is shown. The controller 125 receives information about events and receives signature information to identify the user and type of event 126. Because the controller may be local to the system, the system can function in real time for suspicious events (column 7, lines 55-60)]**, wherein the method further comprises the steps of:

(2) recognizing the need for modification of the access right profiles in the computer system **[i.e., referring to Figure 1, a login anomaly detection function 3 and logout anomaly detection function 7, they are for "recognizing the need for modification of the access right profiles in the computer system". Referring to Figure 3, if the user is not to be ignored and if**

the user is logging in to the system, the monitor builds/updates the user profile database 22 and updates the active user database as shown in Figure 4 (column 4, lines 41-44). In addition, turning now to Figures 5A and 5B, flow diagrams of the logout anomaly detection function are shown. When a user attempts to logout, the logout anomaly detector 49 goes through a series of steps to process the logout to determine if something has occurred during the user's login time that may indicate a system anomaly. The logout entry for the user is updated in the user profile and the active user database is updated 50 (column 5, lines 40-47)];

(3) reading the information contained in the access right profiles **[i.e., again referring to Figure 3, For each user, a profile is automatically built of the days, times and length of time that the user has logged in. Once a certain threshold number of user logins have occurred for this user to allow for accurate user profiling (usually approximately ten logins, but this can be adjusted by the user), the day and time of the current user's attempted login is compared (that means "reading the information contained in the access right profiles") to that profile. If the current login time differs from the user's login profile, the control function is notified 37 (column 5, lines 22-28)];**

(4) establishing which access right profiles have to be modified **[i.e., referring to Figure 1, a local controller function 6, that is for "establishing which access right profiles have to be modified". In fact, referring to Figure 8, the controller 125 receives information about events and receives signature information to identify the user and type of event 126. Because the controller may be local to the system, the system can function in real time for suspicious events. In addition, if the controller is local, the intrusion detection system can be located entirely within the local host computer. The controller then determines the action to be taken and takes appropriate action 127. The action may be to log the event to the local system log 128, log the event to a remote system log 129, disable the user's account 130, block access to the attacking host system address 131, trigger a user defined event 132, drop the**

route to the offending system 133, block network access from the offending system 134, notify the system administrator 135, to ignore the event 136 or any combination of these actions (column 7, lines 55-67 through column 8, lines 1-3)]; and

(5) modifying the access right profiles dynamically as necessary in view of the need for modification that has been recognized **[i.e., the user profile data (signature) is saved and updated every time the user logs on and off the system. The advantage of dynamically building user profile data based on past user behavior and comparing it to that user's current behavior is that the number of false alarms is reduced. In addition, there is no need to enter sets of rules prior to system initialization (column 2, lines 46-52)].**

b. *Referring to claim 2:*

i. Rowland further teaches:

(1) wherein an access right profile comprising one or more user identifiers is defined in the computer system **[i.e., there is a need to automatically build profiling data specific for each user or class of users, that is "one or more user identifiers", that can be used to determine normal actions for a user to reduce the occurrence of false alarms and to improve detection (column 2, lines 22-26)].**

c. *Referring to claim 3:*

i. Rowland further teaches:

(1) wherein an access right profile comprising one or more terminals is defined in the computer system **[i.e., referring to Figure 9, the central system computer 150 may be part of a network that contains multiple host computer (1 through N) 151-153. Each host 151-153 comprises a local controller that sends information about log auditing, login anomaly detection, logout anomaly detection, session monitoring and port scan detector functions to the central controller (column 8, lines 10-16)].**

d. *Referring to claim 4:*

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified as a function of time **[i.e., the odd login time module 184 monitors user logins and attempts to spot "unusual" login times based on past data collected for this user. Odd login times are one of the primary indicators of unauthorized system intrusion. The odd login time module 184 runs only after a predetermined amount of user logins have been collected by the user database. This amount defaults to ten logins, but can be adjusted by the user or system administrator to begin comparing login times after any amount has passed, although sufficient time should be granted to allow accurate profiling (column 9, lines 21-30)].**

e. *Referring to claim 5:*

i. Rowland further teaches:

(1) wherein-the access right profiles in the computer system are modified as a function of the utilization rate of the computer system **[i.e., the theory of operation to take the average login hours from the login tracking field for a particular user. This average is used to draw conclusions about the user's login habits including the days they log into the computer, the times they log into the computer and how long they stay logged into the computer (column 9, lines 31-36)].**

f. *Referring to claim 6:*

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified when a predetermined alarm situation occurs in the computer system **[i.e., The odd login time module 184 runs only after a predetermined amount of user logins have been collected by the user database. This amount defaults to ten logins, but can be adjusted by the user or system administrator to begin comparing login times after any amount has passed, although sufficient time should be granted to allow accurate profiling (column , lines 24-30)].**

g. *Referring to claim 7:*

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified as a function of session duration and/or operation commands used and/or number of sessions held **[i.e., the theory of operation to take the average login hours from the login tracking field for a particular user. This average is used to draw conclusions about the user's login habits including the days they log into the computer, the times they log into the computer and how long they stay logged into the computer (column 9, lines 31-36)].**

h. *Referring to claim 8:*

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

i. *Referring to claim 9:*

i. Rowland further teaches:

(1) wherein the computer system is a telephone switching system **[i.e., referring to Figure 1, "a telephone switching system" is considered to include in the central system controller 150 as shown in Figure 9].**

j. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

k. *Referring to claim 11:*

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

l. *Referring to claim 12:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

m. *Referring to claim 13:*

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

n. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

o. *Referring to claim 15:*

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

p. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

q. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Response to Argument

3. Applicant's arguments filed March 31, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"The system disclosed in Rowland is considerably different than the claimed invention. Rowland is a system for modifying user profile data, whereas the claimed invention is a method for dynamically recognizing and modifying access right profiles. The user profile data in Rowland is not the equivalent of the access right profiles discussed in the claimed invention. The user profile in Rowland is simply a description of the user and their normal activities. Claim 1 in the pending application, however, includes the step of "defining in the computer system access right profiles having individual command rights to the operating system of the computer system." The access right profile in the pending application includes data defining command class-specific powers, validity period of the password, and level of access to the MML command log. The user profile of Rowland does not contain access controls or run rights for commands; rather it merely describes the user's behavior while they are logged on to the system. Thus, the access right profiles recited in the claimed invention is not disclosed in the cited prior art."

Examiner maintains that:

Rowland teaches all the claimed subject matter. Referring to Figure 7, a flow diagram of the session monitoring function 90 is shown. For each user, the

session monitor continuously monitors user activity for a threat to the computer system 91. It continuously monitors the user command entries 92 (that is dynamically recognizing access right profiles), the system process accounting records 93, and commands entered by the user as stored in the user's command history file 94. It compares the command entries 92, system process accounting records 93 (that is modifying access right profiles) and commands in the user's command history file to known threat events and known attack patterns indicating a computer intrusion 95. If a match occurs 96, information and notification is sent to the control function 97. In either case the continuous session monitoring process continues its dynamic monitoring at step 91 (column 7, lines 41-54).

Applicant further argues that:

"Another significant element of the claimed invention, which is not taught by Rowland, is the manner and timing of the modification to the access right profile."

Examiner maintains that:

Rowland's invention teaches the theory of operation is to take the average login hours from the login tracking field for a particular user. This average is used to draw conclusions about the user's login habits including the days they log into the computer, the times they log into the computer and how long they stay logged into the computer. This data can be obtained because the login stamp for each login tracking entry is dynamically maintained by the login monitoring process. Because the database is dynamically generated the signature can be built with intelligence to take advantage of this fact to reduce false alarms. This relieves the administrator of having to setup predefined login profiles for users. This is a great benefit if you have an eclectic user base who work strange hours or login from multiple time zones. The values derived are obtained by calculating the days/hours/minutes (column 9, lines 31-46).

Applicant further argues that:

"The solution set out by the claimed invention first determines the access right profiles, which include unique command rights to the display system of the computer system. Such an access right profile is not disclosed in Rowland."

Examiner maintains that:

Rowland teaches all the claimed subject matter. Besides, the terminology "unique command rights" that the applicant addressed in the remarks does not even include in the claimed language.

Applicant further argues that:

"Independent claim 10 includes a "means for recognizing the need for modification of the access right profiles in the computer system." For instance, this feature can be utilized to prevent the running of commands that are resource intensive at a time when the system is congested; thereby preventing further overload of the system. Rowland, on the other hand, simply changes the user profile every time the user logs into or out of the system. This element in Rowland clearly does not correspond to the modification of the access right profile in the claimed invention. Thus, this element of the claimed invention is not disclosed by the cited prior art.

Examiner maintains that:

Rowland teaches all the claimed subject matter. Besides, the applicant's description: "this feature can be utilized to prevent the running of commands that are resource intensive at a time when the system is congested; thereby preventing further overload of the system" that mentioned in the remarks again does not even addressed in the claimed language.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date

of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
June 2, 2004

LY V. HUA
PRIMARY EXAMINER